PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	)	Confirmation No. 2863
	)	
Johnson	)	Group Art Unit: 2137
	)	
Serial No.: 10/085,895	)	Examiner: Pearson, David J.
	)	
Filed: February 28, 2002	)	HP Docket: 10017900-1
	)	TKHR Docket: 50830-1430
	)	
For: **System and Method for Authenticating Session and Other Transactions**	))	

APPEAL BRIEF UNDER 37 C.F.R. §41.37

Mail Stop Appeal Brief - Patents
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This is an appeal from the decision of Examiner David Pearson, Group Art Unit 2137, mailed January 31, 2008, rejecting claims 1-28 of the present application and making the rejection FINAL.

I. REAL PARTY IN INTEREST

The real party in interest of the instant application is Hewlett-Packard Development Company, a Texas Limited Liability Partnership having its principal place of business in Houston, Texas.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF THE CLAIMS

Claim 1-28 are pending in this application, and all claims were rejected by the FINAL Office Action and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

There have been no claim amendments made after the Final Office Action, and all amendments made before the Final Office Action have been entered. Therefore, all claims 1-28 remain pending in their original form. A copy of the current claims is attached hereto as Appendix A.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the claimed subject matter are illustrated in FIGs. 2 through 9 and are discussed in the specification at least at pages 14-30.

Embodiments of the invention, such as those defined by claim 1, define a method for authenticating a Web session (see e.g., FIG. 3 and related description) comprising: receiving a user ID (see e.g., reference number 210 and related description, including p. 17, lines 1-4); computing a message digest of the user ID (see e.g., reference number 215 and related description, including p. 17, lines 6-11); computing an expiration timestamp for the session (see e.g., reference number 220 and related description, including p. 17, line 11 through p. 18, line 9); selecting an index number (see e.g., reference number 225 and related description, including p. 18, lines 10-11); combining the message digest and expiration timestamp (see e.g., reference number 230 and related description, including p. 18, lines 12-14); accessing an encryption key using the index number (see e.g., reference number 235 and related description, including p. 18, line 15 through p. 19, line 9); encrypting the combined message using the accessed encryption key (see e.g., reference number 240 and related description, including p. 19, lines 10-13); and converting the encrypted message into an ASCII string (see e.g., reference number 245 and related description, including p. 19, lines 13-21).

Embodiments of the invention, such as those defined by claim 17, define a system for authenticating a transaction (see e.g., FIG. 5 and related description, including p. 24, line 19 through p. 25, line 12) comprising: logic configured to receive a user ID (see e.g., reference number 151 and related description, including p. 25, lines 1-2); logic configured to compute a message digest of the user ID (see e.g., reference number 152 and related description, including p. 25, lines 2-4); logic configured to select an index number (see e.g., reference number 154 and related description, including p. 25, lines 4-6); logic configured to combine the message digest with expiration timestamp (see e.g., reference number 155 and related description, including p. 25, line 6); logic configured to select an encryption key from a plurality of encryption keys using the index number (see e.g., reference number 156 and related description, including p. 25, lines 8-9); logic configured to encrypt the combined message using the selected encryption key (see e.g., reference number 157 and related description, including p. 25, lines 12-13); and logic configured to convert the encrypted message into an ASCII string (see e.g., reference number 158 and related description, including p. 25, lines 15-16).

Embodiments of the invention, such as those defined by claim 21, define a method for authenticating a transaction (see e.g., FIG. 6 and related description, including p. 26, lines 3-12) comprising: computing a message digest of a user ID (see e.g., reference number 215 and related description, including p. 17, lines 6-11); concatenating the message digest with an expiration timestamp (see e.g., reference number 315 and related description, including p. 26, lines 5-6); selecting an index number (see e.g., reference number 325 and related description, including p. 26, lines 6-7); selecting an encryption key from a plurality of encryption keys using the index number (see e.g., reference number 335 and related description, including p. 26, lines 7-8); encrypting the message digest using the selected encryption key (see e.g., reference number 340 and related description, including p. 26, lines 8-9); and converting the encrypted message into an ASCII string (see e.g., reference number 345 and related description, including p. 26, lines 10-12).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The FINAL Office Action rejected claims 17-20 under 35 U.S.C. 101 as allegedly being directed to non-statutory subject matter.

The FINAL Office Action rejected claims 1-2, 4-5, 8-13, and 17-24 under 35 U.S.C. § 103(a) as allegedly unpatentable over Reiche (U.S. Patent 6,092,196), and further in view of Bothers (U.S. 2002/0083178).

VII. ARGUMENT

Claim 1-28 are pending in the present application, and all claims stand rejected. For at least the reasons set forth below, Applicant respectfully submits that these rejections should be overturned.

The FINAL Office Action rejected claims 17-20 under 35 U.S.C. 101 as allegedly being directed to non-statutory subject matter

The Office Action asserted rejections under 35 U.S.C. § 101 for the first time during the prosecution of this application, after the previous Appeal Brief. Specifically, the Office Action has rejected claims 17-20 under 35 U.S.C. § 101, as allegedly being non-statutory. In the FINAL Office Action, the Examiner suggested that Applicant amend the claims to recite the additional element of: "a computer storing in a computer readable medium." Applicant appreciates the Examiner's suggestion in this regard and would have been agreeable to such an amendment had the other rejections been withdrawn. However, as the claims remain rejected based on prior art, and as Applicant believes the current claims are in good and proper form (in satisfaction of 35 U.S.C. § 101), Applicant has elected to appeal this rejection.

In this regard, the Examiner's rejection is inconsistent with the U.S. Patent & Trademark Office's treatment of countless other applications. Indeed, the U.S. Patent & Trademark Office has issued numerous patents with this very "logic" claim language (see e.g., U.S. patent 7,296,283 – issued on Nov. 13, 2007: claim 1 defining "logic to authorize ..."). The undersigned sees no relevant difference (from a 35 U.C.C. § 101 perspective) between the claim language issued in that patent and the claim language at issue in this application. In accordance with the Administrative Procedures Act, the U.S. Patent Office (as an administrative agency) cannot act in an arbitrary and capricious manner, and must treat all Applicants equally. The rejection of claims 17-20 in this application is inconsistent with such a policy.

Furthermore, in responding to the previous Office Action, Applicant requested the Examiner to clarify why this rejection had not been made previously. As these claims have never been amended since their original filing with this application, Applicant is confused as to why this rejection was not made prior to the previous appeal filed in this application. As the statutory language of 35 U.S.C. § 101 has not changed, Applicant requested the Examiner to clarify if the Patent Office's construction of this statutory provision has changed, or if the initial examination of these claims was not conducted in accordance with MPEP 707.07(g) (*i.e.*., "Piecemeal examination should be avoided as much as possible. The examiner should ordinarily reject each claim on all valid ground available ..."). The FINAL Office Action did not respond to this inquiry.

In short, Applicant submits that claims 17-20 are in full and proper compliance with the statutory requirements of 35 U.S.C. § 101, as is reflected by other patents being issued with similar "logic configured ..." language, and as is further reflected by the Examiner's failure to reject these claims during the initial examination phase of this application. Consequently, Applicant respectfully requests that the rejection of claims 17-20 be overturned.

The FINAL Office Action rejected claims 1-2, 4-5, 8-13, and 17-24 under 35 U.S.C. § 103(a) as allegedly unpatentable over Reiche, and further in view of Bothers

As set forth above, the FINAL Office Action rejected claims 1-2, 4-5, 8-13, and 17-24 under 35 U.S.C. § 103(a) as allegedly unpatentable over Reiche, and further in view of Bothers.

Independent claims 1, 17, and 21

The present application contains three independent claims: claims 1, 17, and 21. The Office Action has rejected each of these claims under 35 U.S.C. § 103(a) as allegedly unpatentable over the combination of U.S. patent 6,092,196 to Reiche in view of U.S. published application 2002/0083178 to Brothers. For at least the following reasons, Applicant disagrees.

As an initial matter, Applicant notes that the presently pending claims have not been amended during the prosecution of this application, and the present rejections are based on references that were cited in response to a previously-filed appeal brief. The

Office Action that first set forth these new references stated that the new grounds of rejection were made "in view of the Appeal brief." The previous appeal brief, however, merely repeated arguments that had been previously made to the examiner. It therefore appears that the initial search and examination was not fully conducted in accordance with MPEP 904.02 et seq. Despite Applicant's request that the Examiner clarify this point, the FINAL Office Action appeared to have ignored this request, merely stating that Applicant's arguments were not persuasive.

On a substantive basis, with regard to independent claim 1, claim 1 recites:

> 1. A method for authenticating a Web session comprising:
> receiving a user ID; computing a message digest of the user ID;
> computing an expiration timestamp for the session;
> ***selecting an index number***;
> combining the message digest and expiration timestamp;
> ***accessing an encryption key using the index number;***
> ***encrypting the combined message using the accessed encryption key***; and
> ***converting the encrypted message into an ASCII string***.

(*Emphasis added.*) Applicant respectfully submits that claim 1 patently defines over the cited art for at least the reason that the cited art fails to disclose the features emphasized above.

The undersigned submits that there are a number of distinctions in the embodiment of claim 1, but several features are particularly distinctive over the cited art. In addition, the undersigned respectfully submits that the Office Action has taken an overly expansive view of certain claim features in forming the rejection.

To begin, the Office Action admits that Reiche does not teach either: "selecting an index number" or "accessing an encryption key using the index number." However, the Office Action DOES allege that Reiche teaches encrypting the combined message using an encryption key (citing col. 10, lines 21-23). This rejection, however, ignores an expressly claimed feature. In this regard, if Reiche doesn't disclose accessing an encryption key using the index number, then Reiche CANNOT disclose "encrypting the combined message ***using the accessed encryption key.***" Indeed, the cited portion of Reiche (col. 10, lines 21-23) specifically stated that the encryption is performed "using a simple private key encryption algorithm." Consequently, Reiche actually teaches away from a system that provides the security offered by the authentication method of claim 1. For at least this reason, the rejection of claim 1 is deficient and should be withdrawn.

As noted above, the Office Action cites paragraph [0104] of Brothers for disclosing the claimed features of "selecting an index number" and "accessing an encryption key using the index number." Applicant respectfully disagrees. In fact, this cited portion of Brothers teaches:

> [0104] The memory 44 can store an operating system that permits the processor 42 to communicate with the memory 44, communication interface unit 46, the input device 48, the output device 50, and the data storage unit 26, via the bus 52. The memory 44 stores various program modules containing computer code executed by the processor 42 to perform various functions in coordination with the operating system. More specifically, the memory 44 stores a secure URL generator module, an access right enforcer module, a secure caching module, a communication module, and optionally a user authentication module. The memory 44 also stores a secure resource key database that includes key data and resource access right data. Furthermore, the memory 44 can store user authentication data including username/password data in which case the user authentication module performs the functions of the session layer in the ISO/OSI model IEEE specifications. The secure URL generator module is executed in response to a request signal from the WAD 12 requesting a web page document. The request signal can be initially handled by the communication module that manages reception and transmission of signals over the network 18 in coordination with the

> operating system. The secure URL generator module is executed by the processor 42 to retrieve the requested web page document, and to find any URL(s) within the web page document. ***The secure URL generator module retrieves key data and resource access right data for the URL(s) from the secure resource key database. The secure URL generator module secures the resource access right data using the key data.*** If more than one key is used in the system 10, the secure URL generator module can also append key index data indicating the key to be used by the RDS 16 to verify a request to access the resource from the WAD 12. The secure URL generator module combines the resource access right data with its corresponding URL in the web page document. The secure URL generator module calls the communication module that handles transmission of the web page document having URL(s) with resource access right data, to the WAD 12. The access right enforcer module is launched by processor 42 upon receiving a resource request signal from the RDS 16. The access right enforcer module determines whether the RDS 16 is authorized to receive the requested resource. If so, the access right enforcer module calls the secure caching module that retrieves the resource from the data storage unit 26 and retrieves key data corresponding to the RDS requesting the resource. ***The secure caching module encodes the resource with the key data, and calls the communication module to transmit the encrypted resource to the requesting RDS.*** The communication module generates a signal including the encrypted resource and transmits such encrypted resource to the communication interface unit 46 for transmission to the RDS 16. The input device 48 and output device 50 can provide a graphical user interface (GUI) in connection with a server program (not shown) that permits an operator of the web server 44 to perform administrative tasks such as loading or updating the operating system and various program modules, web page document(s), data, and resource(s) stored in the memory 44 and the data storage unit 26.

(*Emphasis added*).

First, Applicant notes that Brothers is not directed to authenticating a Web session, and as such is nonanalogous art to the present application and the system of Reiche. Further, as emphasized above in paragraph [0104], Brothers does not appear to teach "accessing an encryption key ***using the index number***." Instead, Brothers only relevantly teaches that "secure URL generator module secures the resource access right data using the key data." It does not appear to teach accessing an encryption key by using a selected index number.

For at least the foregoing reasons, even if Reiche and Brothers could be properly combined, the resulting combination does not teach all of the claimed features and limitations of claim 1. Consequently, claim 1 patently defines over the combination of Reiche and Brothers. For at least this reason, the rejection of claim 1 should be overturned.

As a separate and independent basis for the patentability of claim 1, Applicant submits that the combination of Reiche and Brothers is improper. In this regard, the Office Action combined selected teachings of Brothers with Reiche to reject claim 1 on the solely expressed basis that "it would have been obvious ... ***because it would increase security because using a different key for each session makes the same log in information appear different for each session, making it more difficult to break the encryption scheme or perform a replay attack.***" (see e.g., Office Action, pp. 4-5). The rationale (or motivation) for the combination, however, was not derived from the prior art itself, but rather from the Examiner's subjective viewpoint of a perceived benefit that would result IF the combination were made.

This rationale is both incomplete and improper in view of the established standards for rejections under 35 U.S.C. § 103.

In this regard, the MPEP section 2141 states:

> Office policy has consistently been to follow Graham v. John Deere Co. in the consideration and determination of obviousness under

> 35 U.S.C. 103. As quoted above, the four factual inquires enunciated therein as a background for determining obviousness are briefly as follows:
>
> (A) Determining of the scope and contents of the prior art;
>
> (B) Ascertaining the differences between the prior art and the claims in issue;
>
> (C) Resolving the level of ordinary skill in the pertinent art; and
>
> (D) Evaluating evidence of secondary considerations.
>
> . . .
>
> BASIC CONSIDERATIONS WHICH APPLY TO OBVIOUSNESS REJECTIONS
>
> When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to:
>
> (A) The claimed invention must be considered as a whole;
>
> (B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination;
>
> (C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention and
>
> (D) Reasonable expectation of success is the standard with which obviousness is determined.
>
> <u>Hodosh v. Block Drug Co., Inc</u>., 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986).

The foregoing approach to obviousness determinations was recently confirmed by the United Stated Supreme Court decision in KSR INTERNATIONAL CO. V. TELEFLEX INC. ET AL. 550 U.S. 1, 82 USPQ 2d 1385, 1395-97 (2007), where the Court stated:

> In Graham v. John Deere Co. of Kansas City, 383 U. S. 1 (1966), the Court set out a framework for applying the statutory language of §103, language itself based on the logic of the earlier decision in Hotchkiss v. Greenwood, 11 How. 248 (1851), and its progeny. See 383 U. S., at 15–17. The analysis is objective:
>
> "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as

> commercial success, long felt but unsolved needs, failure of others, etc., mightbe utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." Id., at 17–18.

Simply stated, the Office Action has failed to at least (1) ascertain the differences between and prior art and the claims in issue; and (2) resolve the level of ordinary skill in the art. Furthermore, the alleged rationale for combining the two references embodies clear and improper subjective hindsight rationale. Furthermore, the two cited references actually teach away from such a combination. In this regard, Reiche specifically teaches "using a simple private key encryption algorithm" (col. 10, lines 22-23) and Brothers is not even directed to Web session authentication. For at least these additional reasons, Applicant submits that the rejection of claim 1 is improper and should be overturned.

With regard to independent claims 17 and 21, those claims are defined by elements that, in all relevant respect, parallel the defining elements of claim 1. Indeed, the Office Action applied the same portions of Reiche (col. 10, lines 14-23) and Brothers (paragraph [0104]) as teaching the claimed features of claims 17 and 21, as were applied to the rejection of claim 1. Furthermore, the Office Action stated nothing additional about the motivation for combining Reiche and Brothers, with respect to claims 17 and 21. Therefore, it is assumed that the rationale for the combination is the same as that advanced in connection with claim 1. Therefore, Applicant submits that the rejections of claims 17 and 21 should be overturned for the same reasons as the rejection of claim 1.

Dependent Claims

Claims 2-16, 18-20, and 22-28 depend from independent claims 1, 17, and 21, respectively and patently define over the cited art for at least the same reasons that these claims contain all limitations of the base claims from which they depend.

CONCLUSION

Based upon the foregoing discussion, Applicant respectfully requests that the Examiner's final rejection of claims 1-28 be overturned by the Board.

In addition to the claims of Appendix A, Appendix B attached hereto indicates that there is no evidence being attached and relied upon by this brief. Appendix C attached hereto indicates that there are no related proceedings.

Please charge Hewlett-Packard Company's deposit account 08-2025 in the amount of $510 for the filing of this Appeal Brief. No additional fees are believed to be due in connection with this Appeal Brief. If, however, any additional fees are deemed to be payable, you are hereby authorized to charge any such fees to deposit account No. 08-2025.

Respectfully submitted,

/Daniel R. McClure/

Daniel R. McClure
Registration No. 38,962

(770) 933-9500

VIII. CLAIMS - APPENDIX

1. A method for authenticating a Web session comprising:

receiving a user ID;

computing a message digest of the user ID;

computing an expiration timestamp for the session;

selecting an index number;

combining the message digest and expiration timestamp;

accessing an encryption key using the index number;

encrypting the combined message using the accessed encryption key; and

converting the encrypted message into an ASCII string.

2. The method of claim 1, wherein the step of combining the message digest and expiration timestamp more specifically includes concatenating the message digest and expiration timestamp.

3. The method of claim 1, further comprises passing the ASCII string to a remote computer using an FTP (file transport protocol) URL (uniform resource locator) within an HTML (hyper-text markup language) page, the FTP URL being of the form ftp://ID:ASCII@hostname, wherein ID is the user ID and ASCII is the ASCII string.

4. The method of claim 1, wherein the step of receiving the user ID more specifically comprises receiving the user ID through an HTML (hyper-text markup language) page that is communicated from a remote client browser.

5. The method of claim 1, wherein the step of computing a message digest of the user ID more specifically comprises computing a four-byte binary value which is an encoded form of the user ID.

6. The method of claim 1, wherein the step of computing an expiration timestamp more specifically comprises computing an expiration timestamp in Epoch format.

7. The method of claim 1, wherein the step of selecting an index number more specifically comprises generating a random number within a predefined range of values.

8. The method of claim 1, wherein the step of accessing the encryption key more specifically comprises retrieving an encryption key from a storage segment containing a plurality of encryption keys, wherein the retrieved encryption key is obtained from a location or position within the storage segment based upon the index number.

9. The method of claim 1, wherein the step of encrypting the combined message more specifically comprises encrypting the combined message digest and timestamp into an eight-byte binary value.

10. The method of claim 1, further comprising the step of concatenating the index number to the encrypted message.

11. The method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically comprises using a "printf" command.

12. The method of claim 1, wherein the step of converting the encrypted message into an ASCII string more specifically includes converting the encrypted message into a hexadecimal value.

13. The method of claim 10, wherein the step of converting the encrypted message into an ASCII string more specifically comprises converting the encrypted message and the index number into an ASCII string using a "printf" command.

14. The method of claim 3, further including the step of passing the index number to the remote computer.

15. The method of claim 14, wherein the step of passing the index number to the remote computer more specifically comprises passing the index number to the remote computer separate from the ASCII string.

16. The method of claim 14, wherein the step of converting the encrypted message into an ASCII string more specifically comprises converting a combination of the encrypted message and the index number into an ASCII string, wherein the index number is communicated to the remote computer as a part of the ASCII string.

17. A system for authenticating a transaction comprising:

logic configured to receive a user ID;

logic configured to compute a message digest of the user ID;

logic configured to select an index number;

logic configured to combine the message digest with expiration timestamp;

logic configured to select an encryption key from a plurality of encryption keys using the index number;

logic configured to encrypt the combined message using the selected encryption key; and

logic configured to convert the encrypted message into an ASCII string.

18. The system of claim 17, further including logic configured to generate an expiration timestamp.

19. The system of claim 17, further including logic configured to communicate the ASCII string to a remote computer.

20. The system of claim 17, further including a local memory for storing the plurality of encryption keys.

21. A method for authenticating a transaction comprising:

computing a message digest of a user ID;

concatenating the message digest with an expiration timestamp;

selecting an index number;

selecting an encryption key from a plurality of encryption keys using the index number;

encrypting the message digest using the selected encryption key; and

converting the encrypted message into an ASCII string.

22. The method of claim 21, wherein the step of encrypting the message more specifically includes encrypting the concatenated message using the accessed encryption key.

23. The method of claim 21, wherein the step of selecting the encryption key more specifically includes retrieving the encryption key from a local memory based on the index number.

24. The method of claim 21, further including the step of communicating the ASCII string to a remote computer.

25. The method of claim 21, further including the step of communicating the ASCII string to a person through voice communication.

26. The method of claim 21, further including the step of printing the ASCII string onto a ticket.

27. The method of claim 26, wherein the ticket is one selected from the group consisting of an airline ticket, a concert ticket, an employee ID card, and an event ticket.

28. The method of claim 26, wherein the step of printing the ASCII string onto a ticket more specifically includes printing the ASCII string onto the ticket in a form that it may be later electronically scanned for verification.

IX. EVIDENCE - APPENDIX

None.

IX. RELATED PROCEEDINGS- APPENDIX

None.